UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,853	11/14/2003	Christopher Lynn Tycho Brown	16666-002001	2765

20985 7590 12/18/2006
FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
PATEL, KAUSHIKKUMAR M	
ART UNIT	PAPER NUMBER
2188	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/18/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/713,853	BROWN, CHRISTOPHER LYNN TYCHO	
	Examiner	Art Unit	
	Kaushikkumar Patel	2188	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 Septemberl 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 7-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 7-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This office action is in response to applicant's communication filed September 29, 2006 in response to PTO office action mailed June 29, 2006. The applicant's remarks and amendments to the claims were considered with the results that follow.

2. In response to the last office action, claims 1, 3, 12, 17 and 36 have been amended. Claims 6 and 37 have been previously canceled. No claims have been added. As a result, claims 1-5, 7-36 remain pending in this application.

3. The previous office action rejection of claims under 35 U.S.C. 112, second par. have been withdrawn due to amendments filed on September 29, 2006.

4. The rejection of claims 1-2, 4-5, 7-8, and 17-20 rejected under 35 U.S.C. 102(b) based upon a public use or sale of the invention is withdrawn due to affidavit filed on September 29, 2006 under rule 37 CFR 1.132 by the applicant.

5. The rejection of claims under 35 U.S.C. 101 is maintained.

Response to Arguments

6. Applicant's arguments with respect claim 1 rejected under 35 U.S.C. 101 has been fully considered but they are not persuasive. Claim 1, cites an article in line 1.

From the current application specification par. [0004], an article is defined as "a machine readable medium". The machine-readable medium further defined as including software products, computer program products, see par. [0018]. Software and program products not embodied by computer readable storage medium are non-statutory and therefore unpatentable.

7. Applicant argues that Stevens teaches a calling process accesses the protected area by locating and using an interface of system firmware. Examiner respectfully disagrees with this. Stevens teaches, "after the computer has been booted, a calling process desiring access to the protected area is caused to locate *an interface that interfaces* **between the calling process and the system firmware**. The calling process is **caused to use the interface** to create a trusted relationship between the calling process and the system firmware" (Stevens, abstract, lines 2-8, par. [0064], lines 1-8). The interface used by the calling process indeed is a device driver, that can be used to access the system firmware command (SETMAX address command, admitted by applicant, see specification, par. [0031], the **kernel mode module 430 to access one or more firmware commands** that do not alter the machine-readable medium.) stored in the hard disk according to PARTIES and BEER specifications (see current application specification, par. [0020], the HPA offers system manufacturers a place to store information and utilities in hidden areas). The interface used by calling process is a device driver running under kernel of operating system (similar to applicant's kernel mode module) and accesses the firmware command SETMAX address command to

reset protected area of the hard disk (similar to applicant's method, as per par. [0031], kernel mode module access one or more firmware commands to remove protection). Thus, it is clear that Stevens uses an interface (device driver, inherently needs loading in the system RAM) running under kernel to locate a firmware (SETMAX address) command to reset protected area of disk, which is equivalent to applicant's kernel mode module loaded in the RAM, locating a firmware command to reset the protected area of the disk. As per applicant's comments with respect comments regarding "BIOS modules are stored in the protected area before booting of the computer" is true and is admitted by the applicant (present application specification, par. [0020[, teaches roles of PARTIES and BEER specifications, and as per present application specification, a firmware command, SETMAX address is stored in HPA with system BIOS, with password protection. Stevens uses an interface (device driver loaded and running under the kernel mode) to create a trusted relationship via a password and then accesses the firmware command SETMAX address to reset protected area of disk. The statement "after the computer is booted" clearly indicated that the calling process (detecting agent) locates the interface (kernel mode module/ device driver to access the firmware command) to establish the trusted relationship to access protected area of disk.

8. With respect to applicant's arguments "a proper motivation to combine Stevens with Adelstien has not been established", the proposed motivation to combine is "to increase the speed of the system" do not provide explanation. Examiner would like to point out that, Stevens teaches accessing a protected area of disk, without rebooting

the system, and hence avoids the delay caused by rebooting the system (rebooting causes the delay is well known in the art) and thus improves the speed of the system. Applicant also argues, Stevens teaches away from the proposed combination with Adelstien, by saying that Stevens emphasizes on BIOS module, but it is clear from above explanation that Stevens provides access to protected area of disk (without rebooting once the system is booted), normally not visible to the operating systems which can be useful to investigate the entire disk.

9. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning (claim 16), it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). And Joy indeed teaches that smaller packets provide faster communication (see Joy, par. [0003], lines 7-9, smaller packets are desirable because there is less latency).

10. Regarding applicant's argument with respect to motivation to combine reference, MPEP § 2144 states, the difference of objective dose not defeat the case for obviousness because, the reason or motivation to modify a reference may often suggest what the inventor has done, but for a different purpose or to solve a different

problem. It is not necessary that the prior art suggest the combination to achieve the same advantage or result discovered by applicant. *In re linter*, 458 F.2d 1013, 173 USPQ 560 (CCPA 1972).

11. Applicant further argues that, Adelstien teaches three different embodiments and there is no suggestion or motivation to combine embodiments to make selection between transport mediums. Examiner would like to point out that applicant's disclosure is not able to provide enough information on selection process. According to present application specification, page 2, par. [0006], "an appropriate communication medium can be selected based on current conditions when the protected area is accessed", par. [0034] states "the detection agent 510 and the detection tool 540 can be designed to communicate over selected transport medium, where a group of multiple transports are supported, for example the transport medium can be selected based on current conditions from a group". It is clear from the above statements that the selection of transport medium is based on the conditions, when the protected area is accessed, but applicant is failed to teach those conditions and it will be difficult for a person of ordinary skill in the art to ascertain the conditions based on which the selection of transport medium is done. At most, the examiner is able understand is that the computer uses multiple transport mediums, such as USB, PCI and network interface medium and detection agent/tool selects one of them but it is not clear why? The only conclusion, examiner was able to ascertain is that when detection tool is local, transport medium that communicates locally (i.e. a bus) is selected and if it is a client/server type

relationship then network communication transport is selected. Also, applicant's specification provides two different embodiments, similar to Adelstien's three embodiments (see present application specification, figs. 4 and 5).

12. Applicant further argues that Adelstein does not teach sending information using packets. Examiner respectfully disagrees with this. Adelstein teaches use TCP/IP protocols to transfer information (Adelstein, pars. [0056], [0068]).

13. Applicant's further arguments with respect to claims 1-37 have been considered but are moot in view of the new ground(s) of rejection.

Specification

14. The amendment filed September 29, 2006 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows:

The propose amendment to specification par. [0018], "software product embodied in computer readable medium" changes the definition of "machine-readable medium" of originally filed disclosure and hence considered as new matter.

Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Rejections - 35 USC § 112

15. The following is a quotation of the first par. of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

16. Claims 11-16, 21-23, 29-30 and 36 are rejected under 35 U.S.C. 112, first par., as failing to comply with the enablement requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Claims 11, 12, 21, 29 and 36 includes a limitation "selecting the transport medium from a group including a peripheral device interface medium and a network communication medium". According to present application specification, page 2, par. [0006], "an appropriate communication medium can be selected based on current conditions when the protected area is accessed", par. [0034] states "the detection agent 510 and the detection tool 540 can be designed to communicate over selected transport medium, where a group of multiple transports are supported, for example the transport medium can be selected based on current conditions from a group". It clear from the above statements that the selection of transport medium is based on the conditions, when the protected area is accessed, but applicant is failed to teach those conditions and it will be difficult for a person of ordinary skill in the art to ascertain the conditions based on which the selection of transport medium is done. At most, the examiner is able understand is that the computer uses multiple transport mediums, such as USB, PCI

and network interface medium and detection agent/tool selects one of them but it is not clear why? The examiner was able to ascertain that when detection tool is local, transport medium that communicates locally (i.e. a bus) is selected and if it is a client/server type relationship then network communication transport medium is selected.

The dependent claims 13-16, 22-23 and 30 also rejected due to deficiency of the parent claims.

Claim Rejections - 35 USC § 101

17. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

18. Claims 1-16 and 18 are rejected under 35 U.S.C. 101. Claim 1, cites an article in line 1 and claim 18 cites machine-readable medium. From the current application specification par. [0004], an article is defined as "a machine readable medium". The machine-readable medium further defined as non-statutory subject matter such as software products, computer program products and statutory subject matter such as storage device, see par. [0018]. Software and program products not embodied by computer readable storage medium are non-statutory and therefore unpatentable.

Applicant is advised to change the term "machine readable medium" to "machine readable storage medium" to overcome the rejection.

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

20. Claims 1-5, 8-15, 17-22, 24, 26-29 and 32-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adelstein et al. (US 2004/0260733 A1) and in further view of Stevens (US 2002/0133702 A1). {(Assaf US 6,728,830 B1, Moore US 2004/0003135 A1, definition of Hardware abstraction layer (HAL) from http://en.wikipedia.org included as supporting documents)}.

As per claim 1, Adelstein teaches an article (figs. 1-4) comprising machine-readable medium (Adelstein, claims) embodying instructions that when performed by one or more machines results in operations comprising:

provides information derived from the storage device area to a data processing system detection tool (Adelstein, pars. [0005], [0021], [0065] and [0069], teaches a detection tool (directly connected to target device or remotely connected via local or wide area network) (a forensic device), which acquires images from portion of disk space and provides information to forensic device);

Adelstein failed to teach detecting and removing the storage area protection. Stevens teaches determining whether a storage device, in a data processing system running an operating system (Stevens par. [0060]), includes a protected area (par. [0009], [0036]), the operating system including a hardware abstraction layer (par.

[0085], teaches use of Windows operating system, and from definition of HAL, it is clear that Windows based operating system includes HAL, Adelstein also teaches Windows operating system, par. [0048]);

removing the storage area protection of the storage device from within the running operating system and without rebooting the data processing system {taught as after an operating system has been booted, a calling process desiring an access to the protected area is caused to locate an interface (device driver, accessing hardware, such as disk drive requires device drivers loaded into memory under kernel of operating system) that permits access to protected area (Stevens, abstract and par. [0064]). These statements clearly indicate processing is executed within the running operating system, removing protection is taught in par. [0074]};

wherein said determining and removing occur in a kernel mode of the data processing system (Steven teaches locating an interface that permits access to protected area to calling process via an interface (par. [0064]). As per present application specification, pars. [0022] and [0023], a kernel mode software module is a device driver that provides access to hard disk drive and an execution of SETMAX command (firmware command, as per present application specification SETMAX command is firmware command, par. [0031] and claim 25) removes protection. Assaf teaches that OS is unaware of protected area and cannot access it without special drivers, such as hard drive commands (IDE commands), see Assaf, col. 5, lines 10-25, the reasoning of establishment of trusted relationship taught by Stevens is also supported by Assaf. Steven further teaches after authentication system firmware moves

SETMAX location, (Stevens, par. [0074]). Thus, Stevens inherently teaches determining and removing occur in kernel mode of data processing system.

It would have been obvious to one having ordinary skill in the art at the time of the invention to use special device driver (kernel mode module) to access protected area of disk as taught by Assaf and Stevens in the system of Adelstein to gain access to protected area of hard disk normally not visible by operating system (well known as per present application specification, background of invention), and thus the system will be able to do complete analysis of hard disk without missing any portion of the disk (Adelstein's system performs regular scanning of disk and as well known in the art the regular scanning performed by Adelstein do not scan protected area of disk) and since removing of storage area protection occurs without rebooting system, increases the speed of the system (rebooting the system imposes a delay).

As per claim 2, Steven and Adelstein teach use Windows operating system (Stevens, par. [0085], Adelstein, par. [0048]), Windows operating system provides function of graphical user interface (GUI), virtual memory management and multitasking (see definition of operating system from http://en.wikipedia.org).

As per claim 3, Stevens teaches checking whether the storage device supports a protected area specification (pars. [0035]-[0036]); and

identifying a protected storage capacity and an unprotected capacity of the storage device (par. [0059]).

As per claims 4 and 5, Stevens teaches removing storage area protection by resetting a storage address value (claim 4) by calling MAX ADDRESS command (pars. [0059] and [0074]).

As per claim 8, Stevens teaches scanning the formerly protected area and identifying file system information in formerly protected area (pars. [0081] and [0084]). Adelstien also teaches scanning hard disk and deriving information from disk (Adelstein, pars. [0065] and [0069]).

As per claim 9, Adelstien teaches sending information to local or remote forensic device (Adelstein, pars. [0043], [0053] and [0054]), which inherently require sending information over transport medium.

As per claim 10, Adelstein teaches reconstructing a file system of storage device (Adelstein, pars. [0065] - [0069]). Also reconstruction of file system is well known in the art (see, present application specification, background of art section, manual reassembly of any file data is then performed, mere making any method automatic is not given any patentable weight).

As per claim 11, With respect limitation "selecting between multiple transport medium" is unclear as explained above with rejection of claim under 35 U.S.C. 112, first

paragraph. Accordingly, Examiner was able to ascertain that, computer systems support multiple transport mediums and while Adelstein teaches connecting forensic device many different ways, Adelstein teaches selecting the transport medium from a group including a peripheral device interface medium and a network communications medium because it is inherent that when agent component running in client/target machine it must send the information to forensic device via a transport medium that was used to connect forensic device to target device (Adelstein, pars. [0043], [0044], [0053] and [0054], taught as forensic device can be connected to client machine via local area networks, wide area networks or directly connected and interrogation agents sends collected data to forensic device).

Claim 12, is similar in scope with combination of claims 1 and 9-11. Thus claim 12 is rejected under same rationales as applied to claims 1, 9-11 above (Adelstein teaches system configured to send information through different kinds of connections (Adelstein, pars. [0053]-[0057]) and through LAN, WAN using TCP/IP protocols, par. [0068], which teaches sending information using packets. Also sending information to forensic device through LAN, WAN using TCP/IP protocols requires network interface card (NIC) connecting target device to network, which inherently requires protocol must be usable over both peripheral interface medium (NIC card) as well as network communication medium (wires).

As per claim 13, Adelstein teaches sending information using universal serial bus (USB) (par. [0054]) and Internet Protocol (IP) (par. [0056]). Sending information over particular transport medium inherently requires packet structure usable over that transport medium.

As per claim 14, Adelstein teaches using host name and target IP address. (Data packets are known to include packet identifier, sender identification and destination identification (detection-tool identification)).

With respect to limitation of claim 15, Adelstein teaches use of TCP/IP as packet transfer protocol as explained with respect to claim 12 above and TCP provides one-to-one connection between two communicating devices.

Claims 17 and 20-21 are similar in scope as claims 1 and 8-10 and rejected under same rationales as applied to claims 1 and 8-10 above. Adelstien teaches scanning disk to derive information from hard drive. The device drivers running under kernel mode provides access to hard disk {see [presented to support examiner's view of device drivers] Moore (US 2004/0003135 A1, pars. [0005] and [0006]) and Assaf (US 6,728,830 B1, column 5, lines 10-25)}. Stevens and Assaf teach a calling process desiring an access to protected area looks for an interface (device driver) to gain access to protected area without rebooting system as explained in claim 1, a device driver must be loaded in system memory in order to be run, thus Stevens inherently teaches loading

kernel mode software module (device driver) without rebooting system. Stevens also teaches removing (as per claim1) and closing protected area (par. [0075]), which teaches reversibly removing the storage area protection. (Shoji et. Al. US 2004/0216141 A1 also teaches utilizing device drivers running under kernel to provide access to hardware, see par. [0015]-[0017], Moore, Assaf and Shoji are introduced here as evidential references to support Examiner's arguments regarding inherency of kernel mode software modules providing access to hardware).

As per claims 18 and 19, Adelstein teaches acquiring evidence from target device without having to pre-load acquisition software on target machine (Adelstein, par. [0047]), which teaches that installation of acquisition software (on hard disk) on target machine is not required. However, Adelstein is silent about method of loading acquisition software, but dynamic loading of software from optical devices into RAM without installing on hard drive is well known in the art and the Examiner takes official notice of that.

As per claim 24, Adelstein teaches a system (figs. 1-3) comprising:

a data processing system detection tool (figs. 1-3, item 12, par. [0042]); and

a kernel mode software module operable to provide the detection tool with access to a protected area of a storage device in a data processing system when the kernel mode software module is loaded into the data processing system (Stevens

teaches accessing protected area of storage device and motivation to combine Stevens with Adelstein is taught with respect to claim 1 above).

As per claim 26, Adelstein teaches forensic device can be directly connected to target device or remotely acquire data through agents (pars. [0003], [0044], [0057]). Thus, Adelstein teaches detection tool as stand-alone and client application.

As per claim 27, Adelstein teaches agents collecting information from target device (par. [0062]), and sending derived information to forensic device, and Stevens teaches accessing protected area of disk requires use of device driver running in kernel mode of the processing system as explained with respect to claims 1, 12 and 24, agent collecting information and sending it to forensic device requires communication between them.

Claim 28 is rejected under same rationales as applied to claim 10 above.

Claim 29 is rejected under same rationales as applied to claims 11 and 12 above.

As per claim 32, Adelstein teaches the detection tool is computer forensic tool (par. [0002]).

As per claim 33, accessing hardware (such as hard disk) require use of device driver, Adelstein teaches scanning hard disk (par. [0065]), thus Adelstein teaches device driver.

As per claim 34, Adelstein teaches Windows operating system (par. [0062]. Windows Deriver Model (WDM) is a component of Windows operating system and thus Adelstein teaches WDM.

As per claim 35, Stevens teaches ATA hard disk (par. [0009]).

Claim 36, is similar in scope to claims 1, 9, 11 and 12 . Adelstein teaches a remote or local detection device (pars. [0003], [0005]) with multi-transport medium (figs. 1-3, pars. [0043], [0053] and [0054]) and provides live imaging (par. [0065]). Stevens teaches removing storage area protection without rebooting system as explained with respect to claims 1, 9, 11 and 12 above. Thus, claim 36 is rejected under same rationales as applied to claims 1, 9, 11 and 12 above.

21. Claims 15, 23 and 30 are rejected under **35 U.S.C. 103(a)** as being unpatentable over Adelstein, Stevens and Assaf as applied to claims 1, 9-11 and 12 above, and further in view of William Stallings (Data & Computer Communications, sixth edition, published, 2000).

As per claim 15, Adelstein, Stevens and Assaf teach limitation of claim 12 above, but fail to packet structure for one-to-one communication. Williams teaches virtual circuit established by packets, which provides one-to-one connection between devices (Williams, pages 307, 311 and 312).

Claims 23 and 30 are similar in scope with combination of claims 14 and 15, and rejected under same rationales as applied to claims 14-15 above.

22. Claim 7 is rejected under **35 U.S.C. 103(a)** as being unpatentable over Adelstein, Stevens and Assaf as applied to claims 1-5 above, and further in view of Rothman et al. (US 2004/0158698 A1).

As per claim 7, Stevens, Adelstein and Assaf teach limitations of claims 1-4 as explained above and further teach closing the protected area (Stevens, par. [0075]) but fail to teach closing protected area by rebooting the system. Rothman teaches that SETMAX ADDERSS command removes protection of storage device volatilely, and hardware reset returns maximum address to last non-volatile settings (Rothman par. [0033]). It would have been obvious to one having ordinary skill in the art at the time of the invention to use system reboot as taught by Rothman in system of Adelstein, Stevens and Assaf to restore storage area protection after accessing the protected area leaving disk in original condition.

23. Claims 16 and 30 are rejected under **35 U.S.C. 103(a)** as being unpatentable over Adelstein, Stevens and Assaf as applied to claims 1, 9-14 and 24-29 above, and further in view of JOY et al. (US 2002/0093982 A1).

As per claim 16, Adelstein and Stevens teaches all limitations of claim 12, but fails to teach small packets. JOY teaches smaller packets (par. [0003]). It would have been obvious to one having ordinary skill in the art to use small packets as taught by JOY in the system of Adelstein and Stevens for faster data transfer (or less latency) (par. [0003]).

Claim 30 is similar in scope with claims 14 and 16, so claim 30 is rejected under same rationales as applied to claims 14-16 above.

24. Claims 25 and 31 are rejected under **35 U.S.C. 103(a)** as being unpatentable over Adelstein, Stevens and Assaf above, and further in view of NIST (National Institute of Standards and Technology) Hard Disk Write Block Tool Specification.

As per claims 25 and 31, Adelstien, Stevens and Assaf teach limitations of claim 24, but fails to teach write blocker. As per requirements of NIST, a write blocker is required in forensics to protect hard disk from unintended modification (see page 3, scope) and requirements of write blocker allows kernel mode software module with read command to operate (see page 5, section 5.1). Hardware and Software are logically equivalent and while hardware is costly to implement but provides faster execution, while software is cheaper. It would have been obvious to one having ordinary skill in the

art at the time of the invention to use write blocker in system of Adelstein to meet the requirements of NIST.

The use of write blocker is also known to person having ordinary skill in the art as per Applicant's announcement for sale of product "ProDiscover DFT" (dated September 10, 2002, "no write accompaniment to ProDiscover DFT for disk drive preview and imaging keeps original evidence safe by write blocking, as evident from applicant's affidavit submitted on September 29, 2006).

Conclusion

25. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaushikkumar Patel whose telephone number is 571-272-5536. The examiner can normally be reached on 8.00 am - 4.30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hyung Sough can be reached on 571-272-6799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kaushikkumar Patel
Examiner
Art Unit 2188

kmp

HYUNG SOUGH
SUPERVISORY PATENT
2/11/06